



DR WOJCIECH RAFAŁ WIEWIÓROWSKI – GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH – WYJAŚNIA

**PYTANIE:**

Czy pracodawca, który pozyskuje dane osobowe w procesie rekrutacji, może je wykorzystywać także w innych celach, np. dla przyszłych rekrutacji lub w celach marketingowych?

ODPOWIEDŹ:

Tak, ale tylko i wyłącznie za zgodą osoby, której dane dotyczą.

UZASADNIENIE:

Zgoda kandydata do pracy na przetwarzanie jego danych osobowych nie jest potrzebna, gdy chodzi o zakres danych wynikający z art. 22¹ Kodeksu pracy. Przepis ten stanowi bowiem podstawę do przetwarzania przez potencjalnego pracodawcę danych osobowych kandydata do pracy obejmujących jego imię (imiona) i nazwisko, imiona rodziców, datę urodzenia, miejsce zamieszkania (adres do korespondencji), wykształcenie oraz przebieg dotychczasowego zatrudnienia. Jest to jednocześnie podstawa prawna z art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych, zgodnie z którym przetwarzanie danych jest dopuszczalne, gdy jest to niezbędne dla zrealizowania uprawnień lub spełnienia obowiązku wynikającego z przepisu prawa. Natomiast jeśli osoba ubiegająca się o zatrudnienie podaje w CV więcej informacji, niż wynika to z ww. przepisów prawa, wówczas podstawą prawną do ich przetwarzania przez potencjalnego pracodawcę jest zgoda tej osoby (czyli podstawa prawna z art. 23 ust. 1 pkt 1 ustawy o ochronie danych osobowych). Taka zgoda jest także wymagana, jeśli dane miałyby być przetwarzane nie tylko w celu rekrutacji, ale także np. w celach marketingowych.

Z punktu widzenia przepisów ustawy o ochronie danych osobowych przez zgodę osoby, której dane dotyczą, rozumie się oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego,

kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie. Formuła zgody na przetwarzanie danych osobowych powinna stanowić odrębne oświadczenie osoby, której dane dotyczą, od innych oświadczeń, z jej treści zaś powinno w sposób niebudzący wątpliwości wynikać, w jakim celu, w jakim zakresie i przez kogo dane osobowe będą przetwarzane.

Przy odbieraniu zgody zagwarantowana powinna być opcjonalność, tj. osoba składająca oświadczenie powinna mieć możliwość wyrażenia zgody na określone działania albo jej niewyrażenia. Z tych względów zgoda na przetwarzanie danych w celach marketingowych powinna być wyodrębniona od zgody na inne czynności. Niedopuszczalne jest także uzależnianie wykonania pewnej usługi czy np. zawarcia umowy od wyrażenia zgody na przetwarzanie danych osobowych w celach marketingowych.

Należy także podkreślić, że na administratorze danych (np. pracodawcy) spoczywa obowiązek dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, poprzez zapewnienie, aby dane były przetwarzane zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane, przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania (art. 26 ustawy).

W związku z powyższym, jeśli kandydat wyraża zgodę tylko na przetwarzanie jego danych w celu przeprowadzenia konkretnej rekrutacji, to oznacza, że po jej zakończeniu jego dane (jeśli nie został przyjęty do pracy) powinny zostać usunięte. Warunkiem ich dalszego przetwarzania w celu np. przyszłych rekrutacji czy w celach marketingowych będzie jego dodatkowa

i wyraźna na to zgoda (na to kto, w jakim celu i w jakim zakresie będzie przetwarzał jego dane osobowe). ■

PYTANIE:

Czy osoby, które w związku z prowadzonym procesem rekrutacyjnym otrzymały od potencjalnego pracodawcy korespondencję wraz z adresami e-mailowymi pozostałych osób, mogą złożyć skargę do Generalnego Inspektora Ochrony Danych Osobowych?

ODPOWIEDŹ:

Tak, gdyż wykorzystywanie adresu e-mailowego bez zgody osoby, której on dotyczy, może stanowić naruszenie ustawy o ochronie danych osobowych.

UZASADNIENIE:

Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych w art. 6 określa definicję danych osobowych. Ustawodawca, formułując art. 6 ustawy, nie określił zamkniętego katalogu informacji stanowiących dane osobowe. Dlatego też przy rozstrzyganiu, czy określona informacja lub informacje stanowią dane osobowe, nieuniknione jest w większości przypadków dokonywanie zindywidualizowanej oceny przy uwzględnieniu konkretnych okoliczności oraz rodzaju środków czy metod potrzebnych do identyfikacji osoby.

Jeśli więc adres e-mailowy stanowi dane osobowe, to jego wykorzystywanie powinno odbywać się z poszanowaniem wszystkich zasad ustawy o ochronie danych osobowych. Jedną z nich jest obowiązek zastosowania przez administratora danych (czyli podmiot decydujący o celach i środkach przetwarzania danych, np. pracodawcę) środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym (art. 36 ww. ustawy). Niewywiązanie się z powyższych obowiązków może w konsekwencji prowadzić do powstania odpowiedzialności karnej na podstawie art. 51 ust. 1 ustawy. W myśl tego artykułu, kto – administrując zbiorem danych lub będąc zobowiązany do ochrony danych osobowych – udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wol-

ności albo pozbawienia wolności do lat 2. Na uwagę zasługuje fakt, że ustawodawca przewidział odpowiedzialność sprawcy również w sytuacji, gdy czyn określony w art. 51 ust. 1 ustawy został popełniony nieumyślnie. Stosownie bowiem do art. 51 ust. 2 ustawy, jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku. Krąg podmiotów określonych w ww. artykule nie został ograniczony wyłącznie do administratora danych, ale obejmuje także inne osoby, na których spoczywa obowiązek ochrony danych, np. pracowników zatrudnionych przy przetwarzaniu danych. W sytuacji gdy mimo podjęcia przez administratora niezbędnych kroków w celu zabezpieczenia danych osobowych, tzn. zastosowania właściwych środków technicznych i organizacyjnych, dojdzie do ich udostępnienia osobie nieupoważnionej, odpowiedzialność ponosi osoba, która wykonywała obowiązki związane z operacjami na danych przetwarzanych przez administratora.

A zatem przy wysyłce korespondencji poszczególne adresy e-mailowe nie powinny być widoczne dla wszystkich adresatów. W przypadku gdy zostaną one udostępnione osobom nieupoważnionym, każda osoba, której dane dotyczą, może złożyć skargę do Generalnego Inspektora Ochrony Danych Osobowych (GIODO). Zgodnie z art. 12 ustawy o ochronie danych osobowych do zadań Generalnego Inspektora należy m.in. wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów tej ustawy. Na podstawie złożonej skargi organ ten może wszcząć postępowanie administracyjne w celu zbadania wszystkich okoliczności faktycznych sprawy i ustalić przez wydanie decyzji, czy doszło w niej do naruszenia przepisów o ochronie danych osobowych. W przypadku zaś takiego naruszenia GIODO nakazuje przywrócenie stanu zgodnego z prawem, a w szczególności usunięcie uchybień (art. 18 ust. 1). Stosownie do art. 17 ust. 2 omawianej ustawy Generalny Inspektor Ochrony Danych Osobowych może żądać wszczęcia postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania przeciwko osobom winnym dopuszczenia do uchybień i poinformowania go, w określonym terminie, o wynikach tego postępowania i podjętych działaniach. ■